

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-357126

(P2000-357126A)

(43) 公開日 平成12年12月26日 (2000. 12. 26)

(51) Int. Cl.

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

テマコード (参考)

3 2 0 F 5 B 0 1 7

審査請求 未請求 請求項の数 6 O L (全 9 頁)

(21) 出願番号 特願平11-169980

(22) 出願日 平成11年 6 月16日 (1999. 6. 16)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外 5 名)

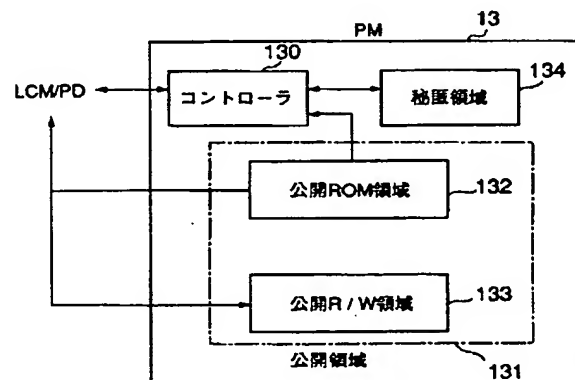
最終頁に続く

(54) 【発明の名称】 記憶媒体及び同媒体を使用したコンテンツ保護方法

(57) 【要約】

【課題】 記憶媒体の特定記憶領域にリボケーション情報が予め登録された構成とすることで、当該記憶媒体がリボケーション情報で表される不当な電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることができるようにする。

【解決手段】 PM (記憶媒体) 13 上に確保された読み出し専用の公開ROM領域 132 に、コンテンツ保護のために無効化すべき PD (記録再生装置) が判別可能なリボケーションリスト RL を予め登録しておき、当該 PM 13 が LCM (コンテンツ利用管理システム) または PD に装着して使用される場合に、PM 13 上に設けられたコントローラ 130 が、その LCM または PD から、その機器を表す情報を受け取って、その情報によりリボケーションリスト RL を参照し、その参照結果に応じて当該機器を無効化するか否かを決定する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域を具備し、

前記記憶媒体が任意の電子機器に装着されて使用される場合に、当該電子機器の無効化を前記リボケーション情報に従って制御可能としたことを特徴とする記憶媒体。

【請求項2】 前記記憶媒体が任意の電子機器に装着されて使用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するコントローラを更に具備することを特徴とする請求項1記載の記憶媒体。

【請求項3】 前記特定記憶領域が、読み出し専用の不揮発性メモリ上に確保された記憶領域であることを特徴とする請求項1記載の記憶媒体。

【請求項4】 前記特定記憶領域が、書き換え可能な不揮発性メモリ上に確保された、秘匿された特定手続以外ではアクセスできない記憶領域であることを特徴とする請求項1記載の記憶媒体。

【請求項5】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体に特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報を予め登録しておき、前記記憶媒体の1つが任意の電子機器に装着されて使用される場合に、前記リボケーション情報に従って当該電子機器の無効化を制御するようにしたことを特徴とするコンテンツ保護方法。

【請求項6】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶メディア部とコントローラとが一体化された記憶媒体のそれぞれに特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報を予め登録しておき、前記記憶媒体の1つが任意の電子機器に装着されて使用される場合に、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するようにしたことを特徴とするコンテンツ保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像データや音楽

データに代表される種々のデジタルコンテンツを記録再生するのに用いられる記憶媒体に係り、特に不当な電子機器によるコンテンツの記録再生を抑止するのに好適な記憶媒体及び同媒体を使用したコンテンツ保護方法に関する。

【0002】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【0003】これらのデジタルコンテンツは、例えばMP3、MP2といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】しかし、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器で用いられる記憶媒体は、別の機器に移動しても記録／再生できるリバーシブルなものが多く、その仕様は基本的にはオープンである。このためコンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは實際上困難である。

【0005】そこで、メモ리카ードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。

【0006】この場合、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化（ライセンス暗号化）／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

【0007】ところが、上記相互認証に必要な情報は、機器の出荷段階で予め設定されていることから、機器の購入後に当該機器（上で動作するプログラム）が改変さ

れるといった攻撃により、例えばコンテンツ保護の仕組みが無効なものになった場合等においては、上記相互認証だけでは、この種の、問題のある機器を検出できないことになる。

【0008】本発明は上記事情を考慮してなされたものでその目的は、特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された構成とすることで、当該リボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能な記憶媒体及び同媒体を使用したコンテンツ保護方法を提供することにある。

【0009】

【課題を解決するための手段】本発明の記憶媒体は、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能であって、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域を備えることで、自身が任意の電子機器に装着されて使用される場合に、当該電子機器の無効化を上記リボケーション情報に従って制御可能としたことを特徴とする。

【0010】このように本発明の記憶媒体においては、その特定記憶領域にリボケーション情報が予め登録された構成とすることで、当該リボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能となる。

【0011】ここで、記憶媒体を、メモ리카ードのように、記憶メディア部とコントローラとが一体化された構成とし、当該記憶媒体が任意の電子機器に装着されて使用される場合に、上記コントローラが当該電子機器から当該電子機器を表す情報を受け取って、その情報によりリボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するならば、記憶媒体側で不当な電子機器によるコンテンツの記録または再生を抑止することが可能となる。

【0012】また、上記特定記憶領域を、読み出し専用の不揮発性メモリ上に確保するか、或いは秘匿された特定手続以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するならば、リボケーション情報の改ざんにも対処可能となる。

【0013】なお本発明は、上記構成の記憶媒体を使用したコンテンツ保護方法としても成立する。

【0014】

【発明の実施の形態】以下、本発明の実施の形態につき図面を参照して説明する。

【0015】図1は本発明の一実施形態に係るコンテンツ利用管理システム1の構成例を示す。なお、ここでは、コンテンツ（デジタルコンテンツ）として音楽デー

タを一例として用いているが、この場合に限らず、映画や、ゲームソフト等のデータであってもよい。

【0016】EMD（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【0017】コンテンツ利用管理システム（以下、LCM（Licence (SDMI-)Compliant Module）と称する）1は、例えば、パーソナルコンピュータ（PC）を用いて実現される。このLCM1におけるコンテンツ保護の方法は、コンテンツを記録すべき記憶メディア（記憶媒体）13毎に、その記憶メディアの識別情報（メディアID）を用いてコンテンツの暗号化／復号化を管理することを前提としている。

【0018】LCM1は、複数のEMD（ここでは、EMD#1～#3）に対応した受信部#1～#3を有しており、当該受信部#1～#3を通してEMDが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号キー）などを受信する。受信部#1～#3は、再生機能や課金機能を有していても良い。また、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【0019】LCM1は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：SMSであり、以下SMSと称する）2を有する。このSMS2は、利用者が購入した暗号化コンテンツをEMD1/F（インタフェース）部3を経由して受け取る。暗号化コンテンツ（ここでは音楽コンテンツ）は、必要に応じてEMD1/F部3で復号され、形式変換や再暗号化が施される。SMS2は暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵（コンテンツ復号キー）をライセンス格納部9に格納する。ここでSMS2は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、SMS2が管理する音楽コンテンツをPC上で再生することができる。

【0020】SMS2はまた、メディア1/F部6に装着可能なメモ리카ード等の記憶メディア（以下、PM（Portable Memory）と称する）13に対してコンテンツデータ（デジタルコンテンツ）を当該1/F部6経由で出力する機能を有している。このPM13は、図2に示す構成の専用の記録再生装置（以下、簡単にPD（Portable Device）と称する）12にセットして用いることで、当該PM13に記録されたコンテンツをPD12上で再生することができる。

【0021】SMS2からPM13へのコンテンツの記録は、メディア1/F部6を通じて直接行われるか、またはPD12を経由して行うことができる。

【0022】ここで、LCM1によるチェックイン／チェックアウト機能について簡単に説明する。チェックアウトとは、LMS1が「親」としてのコンテンツを格納しており、PM13に、その複製を「子」コンテンツと

してコピーすることをいう。「子」コンテンツは基本的にはPD12で自由に再生することが可能であるが、「子」から「孫」コンテンツを作成することは許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、PM13をLCM1のメディアI/F部6に装着し、LCM1が「子」コンテンツを消去（または利用不能）することで、LCM1内の「親」コンテンツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0023】PM13は、図3に示すように、コントローラ130と、公開領域131及び秘匿領域134からなる記憶メディア部とから構成される。秘匿領域134は、コントローラ130を通して非公開の手順（つまり秘匿された特定手段）でしかアクセスできない記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域134は、対応するPM13に固有のメディア識別情報（以下、メディアキーと称する） K_m 等の定数が記憶される秘匿ROM領域と、ライセンスする側から提供される（メディアキーと呼ばれる）秘密データであるライセンス復号キー等の変数が記憶される秘匿R/W（リード/ライト）領域からなる。メディアキー K_m は、各PM13に固有であればよく、シリアル番号や製造番号（PM13個々の製造番号、または製造ロット番号）、他の様々な識別情報を用いることができる。なお、メディアキー K_m を、各PM13に固有な識別情報とライセンス復号キーから生成するようにしても構わない。秘匿ROM領域は例えばROM（読み出し専用の不揮発性メモリ）上に確保され、秘匿R/W領域は例えばフラッシュメモリ（書き換え可能な不揮発性メモリ）の特定領域に確保される。

【0024】公開領域131は、秘匿領域以外の、通常の手順にてアクセス可能な領域であり、読み出し専用の公開領域（以下、公開ROM領域と称する）132と、書き換え可能な公開領域（以下、公開R/W領域と称する）133からなる。公開ROM領域は例えばROM上に確保され、公開R/W領域は例えばフラッシュメモリ上に確保される。この公開ROM領域、公開R/W領域は、先の秘匿ROM領域が確保されるROM、秘匿R/W領域が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【0025】公開ROM領域132には、本発明に直接関係するリボケーション情報が対応するPM13の出荷段階で予め登録されている。このリボケーション情報は、コンテンツの保護のためにPM13の利用を無効化すべき機器（LCM、PD）、更に具体的に述べるならばPM13（内の公開R/W領域133）を対象とするデジタルコンテンツの記録または再生のためのアクセス要求を無効化すべき機器（LCM、PD）が判別可能な情報である。本実施形態において、リボケーション情報

は無効化すべき機器の識別情報（デバイスID）のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストRL」なる用語を用いる。つまり、公開ROM領域132には、リボケーションリストRLが予め登録されている。

【0026】公開R/W領域133には、暗号化されたコンテンツキー（コンテンツ復号キー）、暗号化されたコンテンツ等が適宜記憶される。暗号化されたコンテンツキーは、コンテンツCを復号するための（当該コンテンツCに固有の）コンテンツキー K_c を、PM13に依存するメディアキー K_m で暗号化することで取得されるものである。また、暗号化されたコンテンツ（ここでは2重に暗号化されたコンテンツ）は、 K_c で暗号化されたコンテンツ（ $K_c[C]$ ）をPM13に依存するメディアキー K_m で暗号化する（ $K_m[K_c[C]]$ ）ことで取得されるものである。

【0027】LCM1、PD12もまた、図4に示すようにPM13と同様の記憶領域を有している。即ちLCM1は、公開ROM領域112及び公開R/W領域113からなる公開領域111と、非公開の手順でしかアクセスできない秘匿領域114との各記憶領域を有している。公開R/W領域113には、図1に示す音楽データ格納部10が確保されている。秘匿領域114には、LCM1の識別情報（デバイスID） ID_{LCM} が予め記憶されている。秘匿領域114にはまた、各コンテンツ毎のコンテンツキー K_c が適宜記憶される。秘匿領域114には更に、図1に示す宿帳格納部8が確保されている。SMS2の管理下にある音楽データ格納部10（公開R/W領域113）にて保持される全ての音楽コンテンツは、その識別情報であるコンテンツID（TID）と予め定められた複製可能コンテンツ数、即ち子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼び、（秘匿領域114内の）宿帳格納部8に格納される。LCM1は、SMS2にてこの宿帳格納部8にアクセスするための秘匿された特定の手続が行われた後、宿帳格納部8（を提供する秘匿領域114）からデータを読み取るための秘匿領域ドライバ7を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。

【0028】一方、PD12は、公開ROM領域122及び公開R/W領域123からなる公開領域121と、非公開の手順でしかアクセスできない秘匿領域124との各記憶領域を有している。秘匿領域124には、PD12の識別情報 ID_{PD} が予め固定記憶されている。秘匿領域124にはまた、各コンテンツ毎のコンテンツキー K_c が適宜記憶される。

【0029】図2は、PD12の構成例を示す。PM13は、PD12のメディアI/F部12fに装着して利用される。LCM1がPD12を介してPM13に読み

書きする場合は、LCM1内のPD1/F部5、PD12内のLCM1/F部12e、メディアI/F部12fを経由して当該PM13の秘匿領域134（図3参照）にアクセスする。メディアI/F部12fは、PM13の秘匿領域134にアクセスするための秘匿領域アクセス部（図示せず）を有している。PD12内の公開R/W領域123及び秘匿領域124（図4参照）は、例えばフラッシュメモリ12d上に確保されている。また公開ROM領域122（図4参照）は、ROM12c上に確保されている。このROM12cには、PM13との間で相互認証を行うためのプログラムが書き込まれている。PD12では、CPU12aの制御のもと、このプログラムに従ってPM13との間の相互認証等の処理が実行される。

【0030】次に、本実施形態の動作について、EMDから配信された暗号化された音楽コンテンツをLCM1のEMD1/F部3で受信して、SMS2により音楽データ格納部10に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアI/F部6に装着されたPM13に記録（コピー）するチェックアウト時の動作を例に、図5の流れ図を参照して説明する。

【0031】この場合、チェックアウトの指示が例えばLCM1のユーザインタフェース（I/F）部15を介してなされ、且つPM13がLCM1のメディアI/F部6に装着された段階で、LCM1のメディアI/F部6とPM13のコントローラ130との間で周知の相互認証が行われる（ステップS101）。この相互認証は、LCM1を機器A、PM13を機器Bとすると、次のように行われるのが一般的である。

【0032】まず、機器Aから機器Bを認証するものとする。ここで機器Aは、公開鍵kpを保持しており、機器Bは、機器Aとの間で所定のコンテンツ保護機能を共有しているならば、公開鍵kpに対応する秘密鍵ksを保持している。機器Aは乱数Rを発生して機器Bに送る。機器Bは、機器Aで発生された乱数Rを受け取ると、それを秘密鍵ksで暗号化して、その暗号化された乱数（ks[R]と表す）を機器Aに返す。機器Aでは、公開鍵kpを用いて、ks[R]を復号し、復号結果が先に発生した乱数Rに等しければ、機器Bは正しい相手であると判定する。

【0033】その後、上記と同じことを機器Bから機器Aに対して行うことで、相互認証を行うことができる。この場合、機器Bは公開鍵を保持し、機器Aは秘密鍵を保持し、機器Aが機器Bにて発生した乱数を秘密鍵で暗号化してそれを機器Bで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【0034】以上の相互認証（S101）により、LCM1及びPM13の双方にて正当な相手であることが確認されたとき、LCM1のメディアI/F部6とPM13のコントローラ130との間でキー交換が行われ、同

一の認証鍵（ K_{x1} ）が共有される。このキー交換は、例えばDVD-ROMのコンテンツ暗号化アルゴリズムとして使用されているCSS（Content Scrambling System）に代表されるランダムチャレンジ・レスポンスを用いた方法により行われる。認証鍵（ K_{x1} ）は毎回代わる時変キーである。

【0035】LCM1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身の識別情報ID_{LCM}を読み出して当該ID_{LCM}を認証鍵（ K_{x1} ）で暗号化し、その暗号化されたID_{LCM}（ $=K_{x1}[ID_{LCM}]$ ）をメディアI/F部6からPM13に送る（ステップS102）。

【0036】PM13のコントローラ130は、LCM1側からの $K_{x1}[ID_{LCM}]$ を、先のキー交換で取得した認証鍵（ K_{x1} ）で復号し、ID_{LCM}を得る（ステップS103）。次にPM13のコントローラ130は、復号したLCM1の識別情報ID_{LCM}により公開ROM領域132内のリボケーションリストRLを参照し、当該ID_{LCM}に一致する識別情報が登録されているか否かにより、LCM1によるPM13の利用を無効化するか否かを判定する（ステップS104）。

【0037】もし、ID_{LCM}に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するLCM1によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0038】これに対し、ID_{LCM}に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するLCM1によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキー K_w を読み出し出力する（ステップS105）。そしてコントローラ130は、LCM1のメディアI/F部6との間で（当該LCM1のメディアI/F部6を介して）キー交換を行い、同一の認証鍵（ K_{x2} ）を共有した上で、上記読み出したメディアキー K_w を認証鍵（ K_{x2} ）で暗号化し、その暗号化された K_w （ $=K_{x2}[K_w]$ ）をLCM1に送る（ステップS106）。

【0039】LCM1のメディアI/F部6は、PM13側からの $K_{x2}[K_w]$ を、先のキー交換で取得した認証鍵（ K_{x2} ）で復号し、メディアキー K_w を得る（ステップS107）。次にLCM1のメディアI/F部6は、秘匿領域114に秘匿されているコンテンツキー K_c を取得したメディアキー K_w により暗号化し、その暗号化された K_c （ $=K_w[K_c]$ ）をPM13の公開R/W領域133に書き込む（ステップS108）。

【0040】このように本実施形態では、リボケーションリストRLに従って無効化（リボケート）されたならばPM13から渡されることのない（暗号化された）メディアキー K_w を、当該PM13からLCM1が受け取

って、そのLCM1の秘匿領域114に秘匿されているコンテンツキー K_c を当該メディアキー K_m により暗号化して、PM13の公開R/W領域133に書き込むようにしている。このため、LCM1とPM13との間で認証鍵の交換を行い、その認識鍵を用いてコンテンツキーの暗号化／復号化を行う方法に比べて、リボケーションリストRLで指定される無効化対象LCM（PM13を利用しようとする電子機器）を確実に無効化（排除）できる。なお、LCM1の公開R/W領域113に確保された音楽データ格納部10に蓄積されている暗号化コンテンツ（ K_c [C]）をPM13に送る際に、上記取得した K_m で更に暗号化するようにしても構わない。

【0041】次に、PM13に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作について、図6の流れ図を参照して説明する。まず、再生の指示が例えばPD12に対してなされ、且つPM13がPD12のメディアI/F部12fに装着された段階で、PD12のCPU12aとPM13のコントローラ130との間で（前記ステップS101と同様の）相互認証が行われる（ステップS201）。そして、この相互認

証（S201）により、PD12及びPM13の双方にて正当な相手であることが確認されたとき、PD12のCPU12aとPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵（ K_x ）が共有される。

【0042】PD12のCPU12aは、秘匿領域124に秘匿されている自身の識別情報ID_{PD}を読み出して当該ID_{PD}を認証鍵（ K_x ）で暗号化し、その暗号化されたID_{PD}（= K_x [ID_{PD}]）をメディアI/F部12fからPM13に送る（ステップS202）。

【0043】PM13のコントローラ130は、PD12側からの K_x [ID_{PD}]を、先のキー交換で取得した認証鍵（ K_x ）で復号し、ID_{PD}を得る（ステップS203）。次にPM13のコントローラ130は、復号したPD12の識別情報ID_{PD}により公開ROM領域132内のリボケーションリストRLを参照し、当該ID_{PD}に一致する識別情報が登録されているか否かにより、PD12によるPM13の利用を無効化するか否かを判定する（ステップS204）。

【0044】もし、ID_{PD}に一致する識別情報がリボ

ケーションリストRLに登録されている場合には、コントローラ130は該当するPD12によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0045】これに対し、ID_{PD}に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するPD12によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキー K_m を読み出し出力する（ステップS205）。そしてコントローラ130は、

PD12のCPU12aとの間で（当該PD12のメディアI/F部12fを介して）キー交換を行い、同一の認証鍵（ K_x ）を共有した上で、上記読み出したメディアキー K_m を認証鍵（ K_x ）で暗号化し、その暗号化された K_m （= K_x [K_m]）をPD12に送る（ステップS206）。

【0046】PD12のCPU12aは、PM13側からの K_x [K_m]を、先のキー交換で取得した認証鍵（ K_x ）で復号し、メディアキー K_m を得る（ステップS207）。次にPD12のCPU12aは、PM13の公開R/W領域133に記憶されている暗号化されたコンテンツキー K_c （= K_m [K_c]）を読み込んで、ステップS207で取得したメディアキー K_m により復号し、その復号されたコンテンツキー K_c を秘匿領域124に書き込んで秘匿化する（ステップS208）。したがってPD12では、この復号されたコンテンツキー K_c （と、必要ならば先に復号化したメディアキー K_m と）を利用して、PM13の公開R/W領域133に記憶されている暗号化コンテンツを復号して再生することが可能となる。

【0047】このように本実施形態では、リボケーションリストRLに従って無効化（リボケート）されたならばPM13から渡されることのない（暗号化された）メディアキー K_m を、当該PM13からPD12が受け取って、当該PM13の秘匿領域134に秘匿されている暗号化コンテンツキー（ K_m [K_c]）を、そのメディアキー K_m により復号化して、PD12の秘匿領域124に書き込むようにしている。このため、PD12とPM13との間で認証鍵の交換を行い、その認識鍵を用いて暗号化コンテンツキーの復号化を行うのに比べて、リボケーションリストRLで指定される無効化対象PD（PM13を利用しようとする電子機器）を確実に無効化できる。

【0048】なお、以上の実施形態では、LCM1とPM13の間、PD12とPM13の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報を認証鍵（ K_x ）により暗号化するものとしたが、認証鍵による暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものとするには、認証鍵による暗号化を行うことが好ましい。

【0049】また、以上の実施形態では、リボケーションリストRLが公開ROM領域132に登録されているものとして説明したが、リボケーションリストRLが改ざんされない領域であれば良く、例えば秘匿された特定手続でしかアクセスできない秘匿領域134に登録されるようにしても良い。

【0050】

【発明の効果】以上詳述したように本発明によれば、記憶媒体の特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予

め登録された構成としたので、当該記憶媒体が上記リストで表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンテンツ利用管理システムのブロック構成図。

【図2】図1中のPD（記録再生装置）12のブロック構成図。

【図3】図1中のPM（記憶メディア）13のブロック構成図。

【図4】LCM1、PD12の記憶領域構成例を示す図。

【図5】LCM1からPM13へのコンテンツ記録時の動作手順を説明するための図。

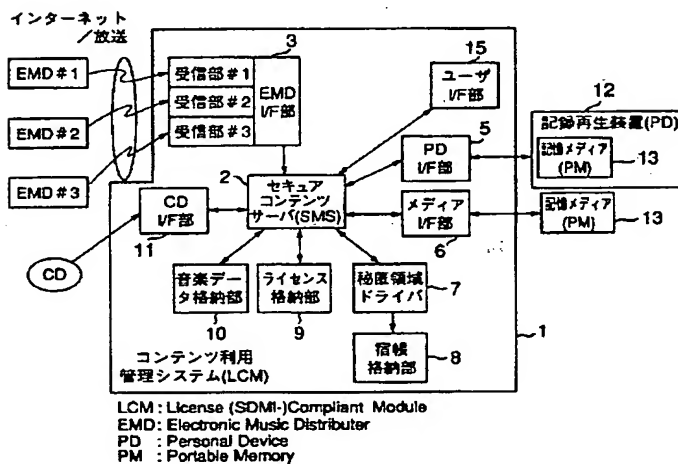
【図6】PM13に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作手順を説明するた*

*めの図。

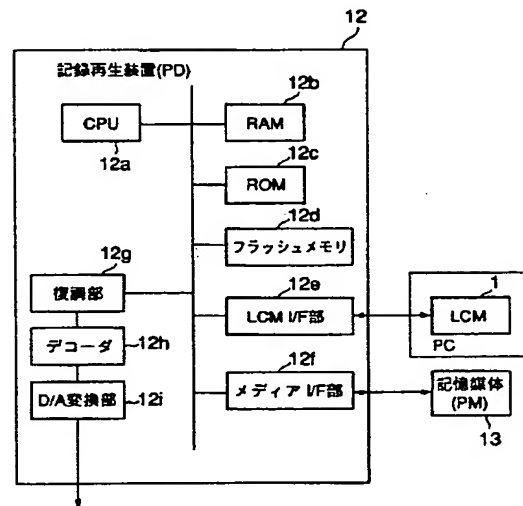
【符号の説明】

- 1…LCM（コンテンツ利用管理システム）
- 2…SMS（セキュア・コンテンツ・サーバ）
- 5…PDI/F部
- 6…メディアI/F部
- 7…秘匿領域ドライバ
- 8…宿帳格納部
- 9…ライセンス格納部
- 10…音楽データ格納部
- 11…CDI/F部
- 12…PD（記録再生装置）
- 13…PM（記憶媒体、記憶メディア）
- 112、122、132…公開ROM領域
- 113、123、133…公開R/W領域
- 114、124、134…秘匿領域
- 130…コントローラ

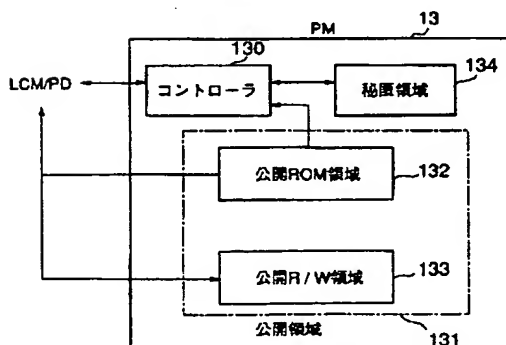
【図1】



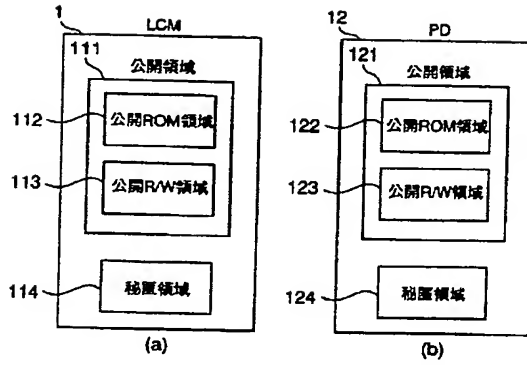
【図2】



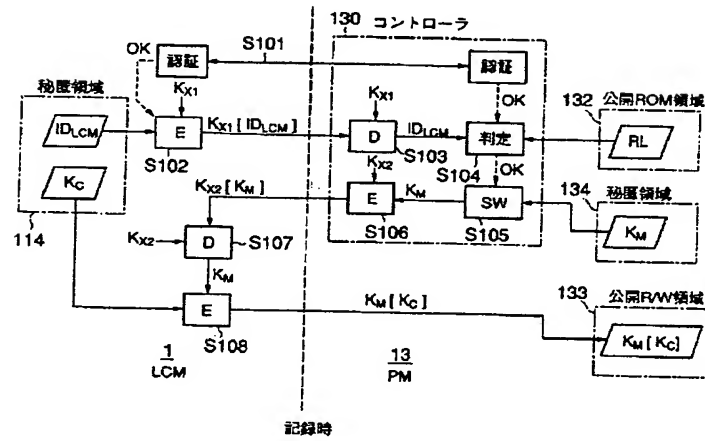
【図3】



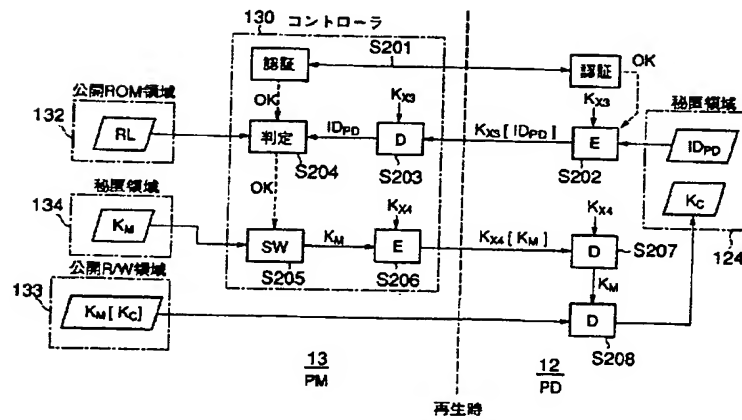
【図4】



【図5】



【図6】



フロントページの続き

- (72)発明者 山田 尚志
東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内
- (72)発明者 岩崎 博
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝マイクロエレクトロニクスセン
ター内
- (72)発明者 田村 正文
東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内
- (72)発明者 石橋 泰博
東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

- (72)発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中工場内
- (72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
- (72)発明者 原田 俊治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
- (72)発明者 勝田 昇
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
- Fターム(参考) 5B017 AA07 BA07 CA15

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)